CLAIMS

What is claimed is:

1. A method for performing blinded ephemeral decryption of a message, the method comprising the steps of:

receiving from a first node at an ephemerizer an ephemeral key ID and a message blinded and encrypted with an ephemeral encryption key of an ephemeral key pair to form a blinded and encrypted message, said ephemeral key pair associated with said ephemeral key ID;

decrypting said blinded and encrypted message using an ephemeral decryption key of said ephemeral key pair to form a blinded message;

communicating said blinded message to said first node; and

irretrievably deleting said ephemeral decryption key in response to a specified event.

2. The method of claim 1 wherein said ephemeral key ID is associated with an ephemeral RSA public and private key pair corresponding to said ephemeral encryption key and said ephemeral decryption key, respectively.

3. The method of claim 1 wherein said ephemeral key ID is associated with an ephemeral Diffie-Hellman key pair having a public key and a private key corresponding to said ephemeral encryption key and said ephemeral decryption key, respectively.

4. The method of claim 1 wherein said ephemeral key ID is associated with a secret ephemeral encryption key and a secret ephemeral decryption key and wherein said secret ephemeral encryption key and said secret ephemeral decryption key are symmetric keys.

ATTORNEY DOCKET NO. P9238
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

5. The method of claim 1 further including prior to the receiving step, the step of generating said ephemeral key ID and said ephemeral encryption and decryption keys of said ephemeral key pair.

6. The method of claim 5 further including the steps of:

receiving a request for an ephemeral encryption key from said first node; and

providing said ephemeral key ID and said ephemeral encryption key of said ephemeral key pair to said first node.

7. The method of claim 6 further including the steps of:

encrypting a message by said first node using said ephemeral encryption key to form an encrypted message;

securely transmitting said encrypted message to a second node.

8. The method of claim 6 further including the steps of:

encrypting said message by said first node using said ephemeral encryption key to form an encrypted message; and

securely storing said encrypted message by a second node.

9. The method of claim 8 further including the step of:

retrieving said securely stored encrypted message by said second node.

10. The method of claim 8 wherein the second node and the first node are the same node.

11. The method of claim 5 wherein said ephemeral encryption key and said ephemeral decryption key of said ephemeral key

ATTORNEY DOCKET NO. P9238
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

pair are an ephemeral RSA public key and corresponding private key, respectively.

12. The method of claim 5 wherein the ephemeral encryption key and said ephemeral decryption key of said ephemeral key pair are Diffie-Hellman public and private keys, respectively.

13. The method of claim 5 wherein said ephemeral encryption key and said ephemeral decryption key of said ephemeral key pair are secret symmetric encryption and decryption keys.

14. The method of claim 5 further including the step of storing said generated ephemeral decryption key on a smart card.

15. The method of claim 14 further including the step of irretrievably deleting said ephemeral key stored on said smart card in response to a specified event.

16. The method of claim 15 further including the step of physically destroying said smart card in response to a specified event.

17. The method of claim 1 wherein said specified event is the recognition of a predetermined date and time.

18. The method of claim 1 wherein said specified event is in response to a request by a user to delete said ephemeral decryption key.

ATTORNEY DOCKET NO. P9238
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

19. A method for performing blind ephemeral decryption of a message M that has been encrypted to form an encrypted message, comprising the steps of:

in a first blinding step, blinding said encrypted message at a first node with a blinding function z to form a first blinded and encrypted message, wherein z has an inverse z^{-1};

in a first communicating step, communicating said first blinded and encrypted message from said first node to a decryption agent;

decrypting said first blinded and encrypted message by said decryption agent using an ephemeral decryption function to form a first blinded message, wherein said ephemeral decryption function is the inverse of said ephemeral encryption function;

in a second communicating step, communicating said first blinded message from said decryption agent to said first node; and

in a first unblinding step, unblinding said first blinded message using z^{-1}, to obtain said message M; and

irretrievably deleting said ephemeral decryption key in response to a specified event.

20. The method of claim 19 wherein said first node and said decryption agent are communicably coupled via a network, and at least one of said first and second communicating steps comprises the step of communicating the respective message over said network.

21. The method of claim 20 wherein said first and second communicating steps comprise communicating the respective messages over said network.

ATTORNEY DOCKET NO. P9238
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

22. The method of claim 19 wherein said first communicating step comprises the step of communicating said first blinded and encrypted message from said first node to said decryption agent via an anonymizer node and said second communicating step comprises the step of communicating said first blinded message from said decryption agent to said first node via said anonymizer node.

23. The method of claim 19 further including the step of rendering said ephemeral decryption function irretrievably deleted upon the occurrence of said specified event.

24. The method of claim 19 further including the step of generating said message at said first node.

25. The method of claim 17 wherein said ephemeral encryption and decryption functions are respectively, ephemeral public and private keys of an ephemeral public key pair.

26. The method of claim 25 wherein said ephemeral public and private keys comprise an ephemeral RSA public/private key pair of the form (e,n) and (d,n) respectively.

27. The method of claim 26 wherein said first blinding step, said blinding function, z, is a number R having an inverse R^{-1} that satisfies $R*R^{-1} = 1 \bmod n$ and wherein said blinding step includes the step of forming the first blinded and encrypted message as the product ($R^e * M^e \bmod n$) where ($M^e \bmod n$) is said message M encrypted using said ephemeral public encryption key.

28. The method of claim 27 wherein the decryption step includes the step of raising the product ((R^e*M^e) mod n) to the

ATTORNEY DOCKET NO. P9238
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

power d mod n, forming $((R^e*M^e) \text{ mod } n))^d$ mod n to form said first blinded message R*M mod n.

29. The method of claim 28 wherein the first unblinding step includes the step of unblinding said first blinded message R*M mod n using R^{-1} to obtain said message M.

30. The method of claim 27 further including the step of generating an integer random number and utilizing said random number as the blinding number R.

31. The method of claim 19 further comprising the steps of:

obtaining an ephemeral public key associated with said decryption agent, wherein said ephemeral public key is a Diffie-Hellman public key of the form g^x mod p;

selecting a blinding number y having an inverse blinding number y^{-1} that satisfies $y*y^{-1} = 1 \text{ mod } p-1$;

raising said public key g^x mod p to the power y to obtain g^{xy} mod p;

raising g to the power y to form g^y mod p;

encrypting said message M using g^{xy} mod p to form an encrypted message of the form $\{M\}g^{xy}$ mod p;

storing a copy of said encrypted message $\{M\}g^{xy}$ mod p; and

storing a copy of g^y mod p.

32. The method of claim 31 wherein the step of decrypting said blinded and encrypted message by said first node includes the steps of:

selecting a blinding number, w having an inverse blinding function w^{-1} that satisfies $w*w^{-1} = 1 \text{ mod } p-1$;

raising said ephemeral public key g^x mod p to the power w to obtain g^{yw} mod p;

ATTORNEY DOCKET NO. P9238
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

forwarding g^{yw} mod to said decryption agent;

receiving g^{xyw} mod p from said decryption agent;

raising g^{xyw} mod p to the inverse blinding number, w^{-1}, to form g^{xy} mod p; and

decrypting said encrypted message $\{M\}g^{xy}$ mod p using g^{xy} mod p to obtain said message M.

33. The method of claim 31 wherein y is a randomly selected integer.

34. The method of claim 31 wherein w is a randomly selected integer.

35. The method of claim 19 including, prior to said first blinding step, the steps of:

selecting a blinding number y having an inverse blinding number y^{-1};

in a second blinding step, blinding said message M using said blinding number y to form a second blinded message;

forwarding said second blinded message to an encryption agent;

encrypting by said encryption agent said second blinded message to form a second blinded and encrypted message, wherein said ephemeral encryption is performed using said ephemeral encryption function and wherein said ephemeral encryption function and said corresponding ephemeral decryption function are secret symmetric ephemeral encryption and ephemeral decryption keys, respectively;

forwarding said second blinded and encrypted message from said encryption agent to said first node; and

ATTORNEY DOCKET NO. P9238
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

in a second unblinding step, unblinding said second blinded and encrypted message using said inverse blinding number y^{-1} to form said encrypted message.

36. The method of claim 35 wherein said second blinding step includes the step of raising said message M to the power y mod p.

37. The method of claim 36 wherein said secret symmetric ephemeral encryption key is a value x and wherein said secret symmetric ephemeral decryption key is x^{-1} and wherein said step of encrypting said second blinded message includes the step of raising said second blinded message M^y mod p to the power x mod p to form said second blinded and encrypted message.

38. The method of claim 37 wherein second unblinding step, includes the step of raising said second blinded and encrypted message M^{xy} mod p to the power y^{-1} mod p, to obtain said encrypted message M^x mod p.

39. The method of claim 38 wherein the step of decrypting said first blinded and encrypted message by said decryption agent includes the step of raising said first blinded and encrypted message to said secret ephemeral decryption key x^{-1} to form a first blinded message M^z mod p.

40. The method of claim 23 wherein said specified event is the occurrence of a predetermined date and time.

41. The method of claim 23 wherein said specified event includes a request by a user to delete said ephemeral decryption key.

ATTORNEY DOCKET NO. P9238
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

42. A system for performing blinded ephemeral decryption of a message, the system comprising:

an ephemerizer communicably coupled to a first node via a communications network;

the ephemerizer operative to;

receive from said first node a blinded and encrypted message, said message being encrypted with an encryption key having a corresponding ephemeral decryption key and said message being blinded with a blinding function to form said blinded and encrypted message;

receive from said first node an ephemeral key ID associated with said ephemeral decryption key;

decrypt said blinded and encrypted message using said ephemeral decryption key to form a blinded message;

communicate said blinded message to said first node; and

irretrievably delete said ephemeral decryption key in response to a specified event.

43. A system for performing blinded ephemeral decryption of a message, the system comprising:

an ephemerizer communicably coupled to a first node via a communications network;

means in said ephemerizer for:

receiving from said first node a blinded and encrypted message, said message being encrypted with an encryption key having a corresponding ephemeral decryption key and said message being blinded with a blinding function to form said blinded and encrypted message;

receiving from said first node an ephemeral key ID associated with said ephemeral decryption key;

ATTORNEY DOCKET NO. P9238
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

decrypting said blinded and encrypted message using said ephemeral decryption key to form a blinded message;

communicating said blinded message to said first node; and

irretrievably deleting said ephemeral decryption key in response to a specified event.

44. A computer program product including a computer readable medium, said computer readable medium having a computer program stored thereon for use in blinded ephemeral decryption, said computer program being executable on a processor in said ephemerizer comprising:

program code for:

receiving from said first node a blinded and encrypted message, said message being encrypted with an encryption key having a corresponding ephemeral decryption key and said message being blinded with a blinding function to form said blinded and encrypted message;

receiving from said first node an ephemeral key ID associated with said ephemeral decryption key;

decrypting said blinded and encrypted message using said ephemeral decryption key to form a blinded message;

communicating said blinded message to said first node; and

irretrievably deleting said ephemeral decryption key in response to a specified event.

ATTORNEY DOCKET NO. P9238
WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313